ABSTRACT

An encryption circuit that reduces a scale of circuit and can achieve a certain level of high-speed processing in the implementation of the AES block cipher. A round processing unit comprises: a first Round Key Addition circuit that adds a round key value to input data; an intermediate register/Shift Row transformation circuit that temporarily stores the output of the first Round Key Addition circuit and executes Shift Row transformation; a Byte Sub transformation circuit into which the values of the intermediate register/Shift Row transformation circuit are inputted and which executes Byte Sub transformation; a second Round Key Addition circuit into which the values of the intermediate register/Shift Row transformation circuit are inputted and which adds round key values; a Mix Column transformation circuit that executes Mix Column transformation upon the outputs of the second Round Key Addition circuit; and a second selector that outputs to the second Round Key Addition circuit one of the outputs of a first selector, the intermediate register/Shift Row transformation circuit, the Byte Sub transformation circuit, and the Mix Column transformation circuit.